Malware Readiness	
"Malware is software that is intended to damage or disable computers and computer systems without the owner's knowledge." *Definition from https://digitalguardian.com/blog/what-malware-definition-tips-malware-prevention, accessed 10 Jun 2019, 0651 EST.*	
Identify	All systems and users are at risk of malware infection. Higher value assets should be hardened against malware first. These could include: • The Cardholder Data Environment (CDE). • Administrative platforms (Active Directory server, network servers). • Customer facing assets (Web Application server, mobile applications). • Customer data (CRM servers, sales lists). • Internal communications and processes (email, Continuous Integration systems).
Protect	User training, data backups, anti-malware software, data encryption, Data Loss Prevention, application whitelisting, firewalls.
Detect	Anti-malware software, point scanners, File Integrity Monitoring, Intrusion Detection (HIDS/NIDS).
Respond	Execute Incident Reponse (IR) plan that allows quick identification of the impact of the malware infection and respond accordingly. Isolate the infected system. Determine the attack vector.
Recover	Patch attack vector, remove virus with anti-malware program from live boot. Remove malware with anti-malware software from live boot. Analyze and implement improvements to system to reduce likelihood of recurrence.

Products for the Malware-Resistant Business

This list is by no means exhaustive and should be considered only a general overview of possible products and their capabilities.

Name	Prevention											Detection								Platform			
	Firewall	Anti-Virus	Anti-malware	Spam Filter	Phishing Protection	Ransomware Protection	Botnet Protection	Shields (Email, Webs)	Sandbox	Patch Management	Full Disk Encryption	Network Monitoring	Application Monitoring	System Monitoring	File Integrity Monitoring	Network Based Intrusion Detection	Host Based Intrusion Detection	Network Based Analytics	User and Entity Behavioral Analytics	Windows	Linux	Mac	Mobile
AT&T Cybersecurity (AlienVault)												✓			✓	✓	✓	✓		✓	✓	✓	✓
ArcSight												✓		✓		✓		✓	✓	✓	✓	✓	
Avast Business Antivirus Pro	✓	✓		✓				✓	✓											✓	✓	✓	✓
Bitdefender GravityZone	✓	✓	✓	✓				✓		✓	✓		✓							✓	✓	✓	✓
F-Secure Client Security Standard	✓		✓			✓	✓	✓		✓									✓	✓	✓	✓	✓
IBM QRadar												✓				✓	✓	✓	✓	✓	✓	✓	✓
McAfee Endpoint Security	✓	✓	✓			✓		✓												✓	✓	✓	✓
Rapid7 (InsightIDR)													✓		✓				✓	✓	✓	✓	
Security Onion														✓	✓	✓	✓	✓			✓		
SolarWinds Threat Monitor										✓						✓		✓					
Splunk																			✓	✓	✓	✓	✓
Symantec Endpoint Protection	✓	✓	✓			✓							✓							✓	✓	✓	✓
Trend Micro	✓					✓						✓			✓			✓		✓	✓	✓	✓

Malware Types	
Adware	Changes configuration of an application, often a web browser, to display annoying advertisements in the form of pop ups.
Backdoor	An unauthorized entry point into the system (i.e. an open port or disguised way of accessing an application) that bypasses usual security mechanisms and can allow attackers access to the system.
Keylogger	Tracks keys user presses to capture sensitive information such as username / password combinations.
Logic Bomb	Set to execute a malicious action at a certain time (i.e. by being placed in Windows Scheduler or a Linux cron job) or when certain system circumstances come true. Often planted by an insider (i.e. a disgruntled IT employee) and difficult to detect.
Ransomware (Crypto-malware)	Denies access to a system or data until a ransom is paid. Usually encrypts the boot drive and demands a cryptocurrency payment to gain the decryption key.
RAT (Remote Access Trojan)	A Remote Administration Tool (also RAT) installed as a Trojan Horse to grant an attacker control of the system, i.e. a Telnet server or Remote Desktop.
Rootkit	Manipulates critical OS files or system memory to hide its existence, making detection difficult.
Spyware	Monitors user activity and used to steal sensitive information. Often bundled into an innocent looking application, such as a game or utility.
Trojan	Opens a back door into the system that a threat actor can use to further exploit the system. Common back doors include open ports and hidden software back doors.
Virus	Spreads through user action, often triggered when an user opens an infected file or plugs in an infected USB stick. Can reduce system performance, fill storage space, render the system unusable or unbootable, infect the boot sector, record information, or be used in conjunction with other malware types.
Worm	Spreads through self replication across the network through instant messages, emails, etc. Can slow down or attack system.